GAO Highlights

FEDERAL FACILITY SECURITY

Selected Agencies Should Improve Methods for Assessing and Monitoring Risk

Why GAO Did This Study

Protecting federal employees and facilities from security threats is of critical importance. Most federal agencies are generally responsible for their facilities and have physical security programs to do so.

GAO was asked to examine how federal agencies assess facilities' security risks. This report examines: (1) how selected agencies' assessment methodologies align with the ISC's risk management standard for identifying necessary countermeasures and (2) what management challenges, if any, selected agencies reported facing in conducting physical security assessments and monitoring the results.

GAO selected four agencies—CBP, FAA, ARS, and the Forest Service— based on their large number of facilities and compared each agency's assessment methodology to the ISC Standard; analyzed facility assessment schedules and results from 2010 through 2016; and interviewed security officials. GAO also visited 13 facilities from these four agencies, selected based on geographical dispersion and their high risk level.

What GAO Recommends

GAO recommends: (1) that CBP and FAA update policies to require the use of methodologies fully aligned with the ISC Standard; (2) that CBP revise its plan to eliminate the assessments backlog; and (3) that all four agencies improve monitoring of their physical security programs. All four agencies agreed with the respective recommendations.

View GAO-18-72. For more information, contact Lori Rectanus at (202) 512-2834 or rectanusl@gao.gov.

What GAO Found

None of the four agencies GAO reviewed—U.S. Customs and Border Protection (CBP), the Federal Aviation Administration (FAA), the Agricultural Research Service (ARS), and the Forest Service—used security assessment methodologies that fully aligned with the Interagency Security Committee's *Risk Management Process for Federal Facilities* standard (the ISC Standard). This standard requires that methodologies used to identify necessary facility countermeasures—such as fences and closed-circuit televisions—must:

1. Consider all of the undesirable events (i.e., arson and vandalism) identified by the ISC Standard as possible risks to facilities.
2. Assess three factors—threats, vulnerabilities, and consequences—for each of these events and use these three factors to measure risk.

All four agencies used methodologies that included some ISC requirements when conducting assessments. CBP and FAA assessed vulnerabilities but not threats and consequences. ARS and the Forest Service assessed threats, vulnerabilities, and consequences, but did not use these factors to measure risk. In addition, the agencies considered many, but not all 33 undesirable events related to physical security as possible risks to their facilities. Agencies are taking steps to improve their methodologies. For example, ARS and the Forest Service now use a methodology that measures risk and plan to incorporate the methodology into policy. Although CBP and FAA have updated their methodologies, their policies do not require methodologies that fully align with the ISC standard. As a result, these agencies miss the opportunity for a more informed assessment of the risk to their facilities.

All four agencies reported facing management challenges in conducting physical security assessments or monitoring assessment results. Specifically, CBP, ARS, and the Forest Service have not met the ISC's required time frame of every 3 years for conducting assessments. For example, security specialists have not conducted required reassessments of two ARS and one Forest Service higher-level facilities. While these three agencies have plans to address backlogs, CBP's plan does not balance conducting risk assessments with other competing security priorities, such as updating its policy manual, and ARS and the Forest Service lack a means to monitor completion of future assessments. Furthermore, CBP, ARS, and the Forest Service did not have the data or information systems to monitor assessment schedules or the status of countermeasures at facilities, and their policies did not specify such data requirements. For example, ARS and the Forest Service do not collect and analyze security-related data, such as countermeasures' implementation. FAA does not routinely monitor the performance of its physical security program. Without improved monitoring, agencies are not well equipped to prioritize their highest security needs, may leave facilities' vulnerabilities unaddressed, and may not take corrective actions to meet physical security program objectives. This is a public version of a sensitive report that GAO issued in August 2017. Information that the agencies under review deemed sensitive has been omitted.

United States Government Accountability Office